AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph [0051], with the following marked-up version of the paragraph:

[0051] Generally, encrypted data sent between client side 350 and server side 360 is encrypted using a tunnel key. The tunnel key can be derived by hashing the concatenation of a Diffie-Hellman shared secret (e.g., session key [[~~131~~]]311) together with client and server nonces. For example, a tunnel key can be derived according to the following formula:

Tunnel Key = HASH [$DH_{ss} + N_c + N_s$]

Please replace the paragraph [0053], with the following marked-up version of the paragraph:

[0053] When client side 350 and server side 360 are performing a negotiation, server request 313 can include negotiation encrypted content 318. Negotiation encrypted content 318 can include challenge 319, authentication method 321, and trust anchor 322. Challenge 319 can be an HMAC of the previous packet ID (e.g., pervious packet ID 314) using a shared secret (e.g., session key [[~~131~~]]311). For example, challenge 319 can be configured according to the following formula:

Challenge = $HMAC_{ss}$[PPid]

Please replace the paragraph [0056], with the following marked-up version of the paragraph:

[0056] When client side 350 is re-authenticating with server side 360 (e.g., authenticating some time after a negotiation), server request 313 can alternately include re-authentication encrypted content 328. Re-authentication encrypted content 328 can include authentication signature 329 and identity certificate 331. Authentication signature 329 can include a signature ID type (e.g., SHA-1 (key ID length = 20 octets) or SHA256 (key ID length = 32 octets)), a signature key ID, and a signature type (e.g., HMAC, RSA PKCS #1, RSA PSS, or DSA). Identity certificate 331 can include, for example, an X.509 certificate, a Kerberos token, a WS-Security token, a Raw Public Key, a hash and URL or an X.509 certificate, a hash and URL of a WS-Security token, a hash and URL of a raw public key.